UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/274,294	03/22/1999	DAVID GUNTER	MS1-298US	8214

22801 7590 01/26/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	14

DATE MAILED: 01/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 14

Application Number: 09/274,294
Filing Date: March 22, 1999
Appellent(s): GUNTER ET AL.

Emmanuel A. Rivera, Reg. No. 45,760
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/24/203.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The amendment after final rejection filed on 7/9/203 has not been entered.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The rejection of claims 1,4, and 2,3, 5-6, 16-18, 20 and 7-15, 19 stand or fall together because Appellant's brief doe not include a statement that this grouping of claims does not stand or fall together and reasons in support of. See 37 CFR 1.192(c)(7).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

5,835,726 Shwed 10-1998

Bruce Schneier, Applied Cryptography, 1996, John Willey & Sons, INC., Second Edition, pg. 31-48

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 4 rejected under 35 U.S.C. 102 (e). This rejection is set forth in prior Office Action, Paper No. 4 and remains rejected in prior Office Action, paper No. 6, under 35 U.S.C. 102(a) as being anticipated by Shwed et al., US Pat. No. 5,835,726,issued November 1998. Shwed is directed to a system for controlling the flow of data packets in computer networks where a security system for inspecting and selectively modifying inbound and outbound data packets is provided, see col. 3 lines 42-63.

As per claim 1, in an embodiment, Shwed discloses that both endpoints (host 1 and host 2) are connected to their respective private networks. Both endpoints are secured via two firewalls (i.e. intermediaries) though their respective networks (i.e. LANs) and are coupled to a public networks, see col. 14, lines 19-39.

Shwed teaches a packet filter module installed in firewalls where modification, inspection of packets is performed by encryption of outbound packets and decryption of inbound packets, see col. 13, lines 6-20. Shwed uses a Deffie-Hellman key generation for a common secret key B which is used to encrypt the session key R. The same session key R is used for both source and destination to encrypt the data from host1 to host2 and from host 2 to host 1, see col. 16, lines 27-31, see also col. 15, lines 34-67 through col. 16, lines 1-4. That is the session key is securely transferred from one of the end points (i.e. either host 1 or host 2) to an intermediary (i.e. firewall 2 or firewall1) by encrypting the session key using secret common key B.

Shwed further teaches that an endpoint (i.e. host 1) in sending a packet M to a receiving endpoint (i.e. a host 2), first it generates a signature on the packet and then encrypts it using a function of session key R (i.e. E=R+I) and finally transmits the encrypted packet (i.e. encrypted data stream) over the public network to the receiver endpoint through a firewall (i.e. an intermediary), see col. 18, lines 9-46.

Shewd further teaches that the firewall in receiving endpoint receives the encrypted packet and verifies (or inspects) the encrypted packet through decryption of the encrypted packet and verification of the signature, see col. 18, lines 47-67 through col. 19, lines 1-3.

As per claim 4, Shwed teaches this, see col. 3, lines 64-67 through col. 4, lines 1-21. In a preferred embodiment, Schwed's method of operating the security system includes a packet filter module implemented as firewall (i.e. an intermediary) which utilizes the stored data from previous inspections to accept or to reject the passage of the data packets into or out of the computer network. That is, the shwed's firewall must have stored the previous data stream in order to be able to perform the comparison for accepting or rejecting the data packet (or. Stream of data).

Claims 2, 3 and 5-6 and 16-18 are rejected under 35 U.S.C. 103(a). This rejection is set forth in prior Office Action, paper No. 4 and remains rejected in prior Office Action , paper No. 6, under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. as applied in claim 1 above, and further in view of Bruce Schneier, Applied Cryptography, Second Edition, 1996, published by John Wiley & Sons, Inc.

As per claim 2, Schwed 's uses 'static" Deffi-Hellman scheme to transfer the session key from the source to the intermediary (i.e. a firewall). The session key R is encrypted using a basic secret common key B which is a function of destination public key, see col. 15, lines 44-67.

However, Schneier teaches a hybrid cryptosystem where public-key cryptography is used to secure and to distribute session key, see pg. 48, lines 8-18.That is, Bob sends Alice his public key. Alice generates a random session key, K, encrypts it using Bob's public key, and sends it to Bob. Bob decrypts Alice's message using his private key. Both of them encrypt their communications using the same session key.

It would have been obvious to one ordinary skill in the art to modify Shwed 's system for controlling the flow of data packets in computer networks to employ Schneier's public key cryptosystem to securely transport the session key (R) from the source (i.e. one end-point) to the intermediary (i.e. the firewall) using intermediary's public key (i.e. the firewall's public key) to take advantage of hybrid cryptosystem in which session key is created when it is needed to encrypt communications and destroyed when it is not longer needed and reducing the risk of compromising the session key, see Schneier, pg. 33, lines 35-40.

Claim 3 additionally recite signing the encrypted session key using a private key associated with one endpoint.

Schneier teaches use of digital signature (i.e. signing a message/data stream or document) with public key cryptography. That is, Alice encrypts the message with her private key and sends the signed message to Bob. Bob decrypts the message with Alice's public key, thereby verifying (or authenticating) the signature, see Schneier, pg. 37, lines 16-30.

It would have been obvious that the source (i.e. host 1) of Shwed signs the session key with its private key to authenticate itself to the firewall (i.e. intermediary), which provides the security of encryption with the authenticity of digital signatures, see Schneier, pg.41,lines 18-30, using sender's private key.

Claim 5 in addition to limitations of claims 1-4 recite that public keys of the endpoints and the intermediary are stored at the key storage and decrypting at the intermediary , the signed encrypted session key using one endpoint's public key to return the encrypted session key and decrypting, at the intermediary, the encrypted session key using the intermediary's private key to return the session key.

The examiner notes the reading of Shwed which suggests that firewall maintains a table of bindings between keys and firewalled network objects (i.e. firewalls and clients). That is, a database (i.e. a key storage) within firewall must be configured so that it knows of other potential firewalls and the hosts' (i.e. endpoints) encrypting firewalls. That is, in order to encrypt communications between firewalls, a firewall must have knowledge of its own basic private key and the basic public keys of each firewalled network object it needs to communicate with, see col. 16, lines 5-26.

Furthermore, Schneier teaches a hybrid cryptosystem where public-key cryptography is used to secure and to distribute session key, see pg. 48, lines 8-18.That is, Bob sends Alice his public key. Alice generates a random session key, K, encrypts it using Bob's public key, and sends it to Bob. Bob decrypts Alice's message using his private key. Both of them encrypt their communications using the same session key.

It would have been obvious to one ordinary skill in the art to modify Shwed 's system for controlling the flow of data packets in computer networks to employ Schneier's public key cryptosystem to securely transport the session key (R) from the source (i.e. one end-point) to the intermediary (i.e. the firewall) using intermediary's public key (i.e. the firewall's public key) to take advantage of hybrid cryptosystem in which session key is created when it is needed to encrypt communications and destroyed when it is not longer needed .

Claim 6 additionally recites a computer readable media at one of endpoints and at the intermediary storing computer-executable instructions for performing the method.

Shwed teaches a storage device (i.e. a computer readable media) at the packet filter module (i.e. a firewall or intermediary) for reading and executing the packet filter instructions, see col. 4, lines 10-21.

the examiner asserts that software is the most obvious vehicle to use for performing functions in a computer. Furthermore, it is well known to use computer readable medium to store software. Official notice is taken of motivation to use software (or instructions) would be to allow either the firewall to perform its functions and the end-points to do the same.

Claims 16-18 are rejected under 35 USC 103 (a) over Shwed and Schneier.

The Examiner assumes such "computer media" and processor to store and to execute computer codes.

Claim 20 is a computer instruction corresponding to claim 1. Claim 20 is rejected.

Claims 7-15 and 19 are allowed over prior art.

Examiner's Statement of Reasons for Allowance

Claim 7 recites " the firewall comprising:

Receiving an encrypted and signed session key from the internal client, the encrypted and signed session key bearing a digital signature of the internal client"

Claim 12 recites :the internal client device being configured to securely transfer the session key to the intermediary".

Claim 19 recites " encrypting the session key at the internal client; signing the encrypted session key to the intermediary; passing the signed and encrypted session key to the intermediary"

Prior art of record fails to teach "encrypting" and "signing" a "session key" at the "internal client" and passing or securely transferring to an intermediary or a firewall as required by independent claims 7, 12 and 19. In prior art, the internal clients are secured by the firewall and that the flow of data steam between an internal client and the firewall is not encrypted. Hence, there is no need for transferring an encrypted session key from an internal client to the firewall (protecting the client).

Dependent claims 8-15 are also allowed by virtue of their dependencies.

(11) Response to Argument.

As per Appellant's arguments relating to the rejection of claim 1, the Appellant Argues that "Shwed does not disclose the environment recited in the preamble; namely, an encrypted data stream being transferred over a network between two endpoints, where the data stream is encrypted using a session key known to both endpoints", page 11 of the Appeal Brief.

The Examiner responds that shwed's invention concerns "an encryption scheme for securing the flow of data over insecure public networks, such as the internet, thus forming a VPN ", see col. 2, lines 62-65 (Shwed). That is, an encrypted data stream being transferred over a network between endpoint " to control information flow by a packet filter capable of examining every packet of information flowing past a node in the system, the packet being encrypted.", see col. 2, lines 37-40 (Shwed).

The Appellant argues that " the endpoints described in shwed are host or client computers 1600 and 1610 and that these computers do not directly exchange data (i.e. communicate) with one another".

The Examiner responds that the Appellant fails to define the claimed "endpoints". The Examiner notes the Appellant of the case (*Intervet America Inc. v. Kee-Vet*

Laboratories Inc., 12 USPQ2d 1474 (CA FC 1989)) which discusses improperly construing a limitation of claim not limited by its recitation in the claim nor limited in the written description and the case (*Bell Atlantic Network Services Inc. v. Covad Communications Group Inc.*, 59 USPQ2d 1865 (CA FC 2001)) which the court affirmed summary judgment of claim construction using the specification as guidance in interpreting the claims.

The Examiner's broadest reasonable interpretation of claimed "endpoints" corresponds to Firewall1 and Firewall 2 of Shwed acting as both intermediaries and endpoints. That is, Firewall1 and Firewall2 both act as secure pathway for host1 and host2 as well as an intermediary to examine the data packet flowing from host 1 to host2 or vice versa. In other words, the Firewall 1 is a source of transmitting encrypted packet(i.e. an endpoint) to intermediary firewall 2, while it is also an intermediary point for inspecting packets received from host2. The Examiner responds that Firewall1with respect to firewall2 (an intermediary) is considered an endpoint while the reverse is also true that the Firewall2 is an endpoint relative to firewall1 acting as an intermediary, see also col. 20,lines 33 through page 23, line13.

The Appellant further argues that Shwed fails to disclose " securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream", page 12 of the Appeal Brief

As stated in the rejection of claim 1 above, Shwed teaches transferring a session key R from Firewall 2 (an endpoint) to Firewall1 (an intermediary with respect to host 1) using common key B using Deffie-Hellman key generation.

As per Appellant's arguments relating to the rejections of claims 2,3,5-6 and 16-18, the Appellant argues that "Shwed does not suggest or teach a session key known to both endpoints", page 13 of the Appeal Brief

The Examiner responds that Shwed's session key R is known to Firewall1 and Firewall2 as clearly addressed in the statement of rejection of claim 1 above.

Appellant further argues that "Schneier provides no teaching of a method for inspecting an encrypted data stream over a network between endpoints when the session key is securely transferred from one of the endpoints to an intermediary", page 14 of the Appeal Brief.

The Examiner responds that Schneier reference is a secondary reference used in a 103 type rejection for the teaching of securely transferring the session key from one endpoint to an intermediary and not for the teaching of "inspecting an encrypted data stream".

As per Appellant's argument relating to the rejection of claim 5, the Applicant argues that the combination of Shwed /Schneier fails to teach or suggest "obtaining , at the intermediary , the one endpoint's public key from the key storage", page 15of the Appeal Brief.

The examiner responds that Shwed teaches a database (i.e. a key storage) within the firewall configured so that it knows of other potential firewalls and the hosts' (i.e. endpoints) encrypting firewalls. That is, in order to encrypt communications between firewalls (as intermediary or endpoint), a firewall must have knowledge of its own basic private key and the basic public keys of each firewalled network object it needs to communicate with, see col. 16, lines 5-26.

As per Appellant's argument relating to the rejection of claim 16, the Applicant argues that Shwed/Schneier does not suggest nor teach " sending the signed and encrypted session key to the intermediary", page 18 of the Appeal Brief

The Examiner responds that Shwed teaches sending encrypted session key from one firewall (endpoint) to another firewall (intermediary) using common secret key B as addressed in the statement of rejection of claim 1 above. Furthermore, Schneier teaches benefits of signing

(i.e. a digital signature) in a hybrid cryptosystem for authentication as addressed in the statement of rejection of claims 2-3 above.

RB

January 20,2003

Conferees

Justin Darrow, Primary Examiner

JUSTIN T. DARROW
PRIMARY EXAMINER

Mathew Smithers, Primary Examiner

Taghi T. Arani, Examiner

Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 50
Spokane, WA 99201

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137